CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

JOSÉ JULIÁN JARAMILLO POVEDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
TULUÁ
2020

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

JOSÉ JULIÁN JARAMILLO POVEDA

ACTIVIDAD ETAPA 5

M.Sc. JOHN FREDDY QUINTERO
DIRECTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
TULUÁ
2020

CONTENIDO

pág.

RESUMEN

En el presente trabajo se encontrará una descripción de cada una de las etapas realizadas en el seminario especializado durante el desarrollo del mismo. De igual manera se expresaran los logros alcanzados y se propondrán acciones o recomendaciones que pueden ser tenidas en cuenta para el mejoramiento de futuros cursos de este seminario.

GLOSARIO

BLUE TEAM: equipo de profesionales en seguridad informática que usa la información aportada por el Red Team para mejorar los niveles de seguridad digital de una empresa.

CVE: es el acrónimo de Common Vulnerabilities and Exposures – Vulnerabilidades y Exposiciones Comunes. Es un listado en el cual se encuentran identificadas con un código las vulnerabilidades detectadas para un sistema (base de datos, sistema operativo, aplicación, Etc.). Por ejemplo la CVE-2017-0144 se refiere a la vulnerabilidad para Windows 7 que hizo posible el ataque con Wanna Cry. La lista total de CVEs puede ser encontrada en : https://cve.mitre.org/

EXPLOIT: se designa a una vulnerabilidad que puede ser usada para atacar a un sistema, por medio de la ejecución de un código, script o programa.

GPL: acrónimo de General Public License – Licencia General Pública. Tipo de licenciamiento de muchos programas, aplicativos, sistemas operativos, Etc. que brinda al usuario la posibilidad de usar un programa sin tener que pagar por derechos de autor.

ISAAF: es una metodología de intrusión creada con el fin de proporcionar un marco definido para la realización de un pentesting.

MALWARE: tipo especial de software, aplicativo o programa en el cual se agrupan todos aquellos que buscan generar algún tipo de perjuicio a la máquina en la cual se están ejecutando. Algunos ejemplos de estos pueden ser: virus, caballos de troya, gusanos, Etc.

OWASP: es un acrónimo de Open Web Aplication Security Proyect – Proyecto Abierto de seguridad en aplicaciones Web - Es un proyecto liderado por Open Source Foundation que busca mejorar el nivel de seguridad de las aplicaciones web, determinando y corrigiendo las causas que pueden hacerlas inseguras.

PENTESTING: conjunto de actividades, realizadas de forma metodológica y ordenada en un sistema informático por un pentester, a fin de detectar la mayor cantidad de vulnerabilidades posibles y generar estrategias de seguridad que remedien o contrarresten estas brechas de seguridad.

RANSONWARE: un tipo especial de malware que, una vez ejecutado en un sistema, realiza la encriptación de la información almacenada en el, tras lo cual generalmente se exige el pago de un rescate a fin de liberar la clave con la que se puede desencriptar y recuperar la información

RED TEAM: equipo de profesionales en seguridad informática que realiza pruebas de intrusión en un entorno definido (generalmente la red de una empresa) a fin de detectar vulnerabilidades que pudieran ser explotadas por un atacante real.

INTRODUCCIÓN

En la actualidad es innegable que el nivel de conectividad a futuro tiende a aumentar de manera continua. Hoy por hoy es posible tener conexión a Internet incluso desde algo tan simple como un reloj inteligente. Cada día se avanza a pasos agigantados en brindar a los usuarios una experiencia mucho más fácil para interactuar con los sistemas; pero esto no solo se enfoca a la conexión a la Web. Existen múltiples redes de comunicaciones, usadas por millones de empresas, para gestionar la información de sus actividades comerciales.

Todo este gran volumen de datos se hace muy atractivos para que un ciberdelincuente pueda sacar provecho en su beneficio. Acciones como Phishing, estafas digitales, ciberataques a empresas, difusión de virus, y un largo Etc. hacen hoy en día totalmente indispensable contar con profesionales altamente capacitados en seguridad digital, que cuenten con un nivel superior de conocimientos de forma tal que puedan brindar seguridad a estos entornos. Pero el conocimiento en si no es suficiente, el profesional debe contar con un gran sentido ético y un conocimiento básico de la legislación aplicable.

En el seminario especializado se brindó al participante una visión holística, de forma tal que en un ambiente real el profesional pueda resolver de la mejor manera un caso presentado.

OBJETIVOS

2.1 OBJETIVO GENERAL

Presentar un informe técnico en el cual se evidencie de manera clara cada una de las etapas realizadas por el estudiante durante el seminario especializado.

2.2 OBJETIVOS ESPECÍFICOS

- Documentar los aspectos más relevantes de las etapas ejecutadas durante el seminario especializado
- Proponer recomendaciones enfocadas a un mejor desempeño del enfoque Red Team & Blue Team
- Concluir cuales son los aspectos más relevantes obtenidos durante el desarrollo del seminario.

PRESENTACIÓN DEL INFORME TÉCNICO

El desarrollo del seminario estuvo dividido en cuatro momentos claves, durante los cuales el participante obtuvo una serie de conocimientos básicos, que aumentando en su complejidad a medida que se avanzaba, lograron que estos se afianzaran por medio de la fundamentación técnica, legal y ética cómo de la práctica aplicada.

Las etapas que se llevaron a cabo fueron:

- Una exploración legal, metodológica y técnica del pentesting y la configuración de ambiente de trabajo
- Una revisión de los aspectos éticos y legales de un contrato de pentesting
- Desarrollo de un ataque desde la perspectiva Red Team
- Contención de un ataque desde la perspectiva Blue Team.

Se realizará una descripción a mayor profundidad de cada una de estas etapas, así como las acciones ejecutadas

3.1 PRIMERA ETAPA

Durante esta se realizó una revisión del estado actual de la jurisprudencia colombiana, en lo concerniente a lo que tiene que ver con delitos informáticos.

Se hizo un análisis detallado de las leyes existentes y se encontró que Colombia ha avanzado mucho en la expedición de normas, leyes y decretos que buscan prevenir, combatir y castigar todos aquellos delitos que se cometen por medio de los dispositivos electrónicos, con la ayuda de estos o que usan la tecnología para la comisión de los ataques.

Con base en la investigación se pueden nombrar las siguientes leyes:

- Ley 1273 de 2008 – “Ley de delitos informáticos”
- Ley 1480 de 2011 – “Ley de protección al consumidor por medios electrónicos”
- CONPES 3701 de 2011 – “Ciberdefensa y Ciberseguridad”
- Ley 1621 de 2013 – “Ley de inteligencia y contrainteligencia”
- Ley 679 de 2001 – “Ley contra la pornografía infantil – Responsabilidad de las ISPs”

De igual manera se indagó por las principales metodologías que se encuentran vigentes en el entorno del pentesting, logrando identificar algunas como: OWASP, ISSAF, OSSTMM, la cuales buscan estructurar de una manera completa los distintos pasos que se deben llevar a cabo durante un proceso y que permitan lograr los objetivos propuestos.

También, y teniendo en cuenta las fases del pentesting, se realizó una indagación sobre algunas herramientas o aplicaciones que pueden ser usadas durante cada una de las fases. Es conveniente aclarar que existen multitud de programas, aplicaciones, distribuciones basadas en Linux, software comercial, Etc. que puede ser utilizado en el desarrollo de un pentesting, pero en este seminario se hizo enfoque en aquellas que cumplieran con las siguientes condiciones: que tuvieran una base reputacional amplia,

es decir, aquellas que son consideradas como buenas soluciones por la comunidad que conoce estos temas; la otra condición es que fueran herramientas libres o con licenciamiento GPL y una última condición es que estuvieran lo suficientemente documentadas, ya que se requiere un buen soporte documental para lograr dominarlas.

Algunas de las que se identificaron son: Nmap, Kali Linux, Backtrack, Metasploit, ExploitDB.

Un último paso fue la configuración de un ambiente de pruebas, con el uso del programa de virtualización Oracle VM Virtualbox, en el cual se crearon 3 máquinas virtuales y se instalaron las respectivas imágenes ISO que fueron entregadas por el tutor.

Una de los sistemas corresponde a Kali Linux, el cual es el programa desde se realizaron las pruebas, otra máquina corresponde a un S.O. Windows 7 a 64 bits y la otra a Windows 7 a 32 bits.

3.2 SEGUNDA ETAPA

Durante el desarrollo de esta etapa, se llevó a cabo el análisis de un modelo de contrato ficticio entre el estudiante y la empresa Whitehouse. El objetivo de este ejercicio fue el de generar en el estudiante el conflicto ético a fin de evaluar sus posturas y postulados de tal manera que pudiera contrastar estos contra un evento.

El contrato presentó una serie de irregularidades las cuales debían ser descubiertas, analizadas y explicadas a profundidad, argumentando las razones por las cuales se estaba o no de acuerdo con ellas, mirándolas desde la óptica legal o desde el campo ético.

Este ejercicio puede decirse que es la aplicación en un caso hipotético de lo aprendido durante la primera etapa.

También se realizó el análisis del caso real “Buggy”, el cual sucedió en la ciudad de Bogotá y en el cual se realizaron actuaciones que rayaban con la ilegalidad y presentaban una serie de conflictos éticos.

3.3 TERCERA ETAPA

En esta se llevó a cabo un ataque real realizado en un ambiente controlado. El ejercicio fue el siguiente: se entregó al estudiante una guía, en la cual se detallaba un caso y por medio del laboratorio de máquinas virtuales creado en el primer estadio del seminario se debía realizar todo el proceso de pentesting.

En el ambiente de pruebas existían dos máquinas con S.O Windows 7, una de las cuales presentaba una fuga de información; el trabajo del pentester era realizar las etapas definidas en el proceso, analizar los ambientes, buscar las vulnerabilidades que pudieran tener, realizar el ataque, acceder a la máquina o máquinas comprometidas y

una vez dentro ejecutar un archivo, con el cual se podía evidenciar el desarrollo del trabajo y finalmente documentar debidamente todo el paso a paso.

Este enfoque se hizo teniendo en cuenta el desempeño de un Red Team, el cual es un equipo de profesionales en seguridad digital que buscan explotar las vulnerabilidades de un sistema a fin de corregirlas.

En este caso en particular, las máquinas eran vulnerables al CVE-2017-0144, el cual es una vulnerabilidad real que en año 2017 permitió que miles de computadores fueran infectadas por el ransonware WannaCry, el cual secuestraba y encriptaba la información del disco duro del equipo comprometido. Otro malware que usó este exploit fue el gusano eternalrocks, el cual se multiplicaba de forma tal que bloqueaba por completo los sistemas afectados.

3.4 CUARTA ETAPA

La aplicación de los conceptos de Blue Team fue el enfoque de esta última etapa. Por medio de la investigación en temas tales como hardening, CIS, CSIRT o SIEM se retó al estudiante a que propusiera las técnicas por medio de las cuales podría realizar la contención de un ataque en tiempo real o prepararse para enfrentarlo.

El hardening consiste en el endurecimiento de un sistema por medio de la revisión, deshabilitación, desinstalación, configuración, Etc. de aquellos puntos vulnerables que puedan ser usados por un atacante en un posible ataque. El hardening busca el justo medio entre seguridad y disponibilidad del sistema.

Por medio de CIS-controls es posible la aplicación de guías con las cuales se mejora la seguridad de un sistema; estas buenas prácticas son propuestas por CIS, la cual es una entidad internacional sin ánimo de lucro, compuesta por expertos en seguridad digital, que buscan luchar contra los ataques cibernéticos.

Los CSIRTs son un tipo de equipo de respuesta de primera nivel el cual busca entre otras cosas detectar los ataques, contenerlos y mejorar la seguridad de un sistema informático, buscando siempre la continuidad del negocio, de tal forma que un ataque tenga el menor impacto posible. Se pueden encontrar a varios niveles (por empresa, región, o incluso nacionales) y comparten conocimiento con otros CSIRTs.

Estos contrastan con los equipos Blue Team, los cuales son enfocados a nivel empresarial y trabajan de forma mancomunada con los Red Team a fin de mejorar los entornos de seguridad.

De igual manera se indagó por la pertinencia de tener un aplicativo SIEM. Este tipo de programas centraliza en una única solución, todos los programas a nivel defensivo que tenga una empresa, de forma tal que se obtenga una vista consolidada de todos los aplicativos, por medio de la estandarización de la información que cada uno de estos entrega. Algunos de los inconvenientes con este tipo de soluciones son su costo, ya que en la actualidad no existen versiones bajo licenciamiento GPL, otra tiene que ver con su impacto sobre una organización de tamaño mediano por que puede que sea un recurso subaprovechado.

RECOMENDACIONES

Una vez realizado el seminario de profundización y como una forma de mejorar la presentación de futuros cursos de este se proponen las siguientes recomendaciones:

- Profundizar en las etapas prácticas, de tal manera que el estudiante pueda adquirir destrezas en diferentes eventos o con distintas herramientas, que pueden ser las más conocidas, de forma tal que se obtenga un nivel óptimo de conocimiento que pueda ser aprovechado.
- Realizar pruebas de Red Team a diferentes ambientes (base de datos, páginas web, servidores, Etc.) por medio de técnicas de pentesting enfocadas a estos, debido a que, dependiendo del tipo de ambiente a explotar, las técnicas pueden variar. No es igual realizar un ataque DDoS a realizar un SqlInyection y sería bueno que se tuvieran las bases de estos.
- Crear un equipo de egresados de la especialización en Seguridad Informática, apoyados por la UNAD, que puedan intercambiar conocimientos de forma regular, participar en eventos o incluso competir entre ellos en un ambiente controlado Red Team & Blue Team, lo cual redundará en el intercambio de conocimiento.
- Estimular la generación de conocimiento con la generación de charlas, seminarios virtuales, eventos, Etc.
- Estudiar la posibilidad de ofrecer en la UNAD la maestría en seguridad informática, de tal manera que los egresados de la especialización puedan profundizar en este apasionante campo.

ENLACE AL VIDEO

De acuerdo a lo solicitado en la guía de actividades de la etapa 5, a continuación, se presenta el enlace al video en el cual el estudiante del seminario realiza la sustentación del trabajo.

https://youtu.be/H-5J4QAkOLU

CONCLUSIONES

- El especialista en seguridad digital debe ser un profesional íntegro, con un excelente dominio de las soluciones informáticas, pero sobre todo poseer una alta calidad ética, ya que debido al nivel de sus conocimientos podría ser usado para fines delictivos.

- Las empresas deben invertir proactivamente en seguridad digital, ya que el nivel de amenazas y ataques está creciendo día a día, máxime en esta época de pandemia donde muchas personas han debido cambiar sus hábitos de estudio, trabajo o diversión.

- La mejor forma de aumentar el conocimiento es compartirlo, ya que de esta forma se pueden contrastar y aprender desde la experiencia del otro. Por lo anterior es bueno formar equipos de egresados que estén en constante interacción.

- Se debe propender por el uso de programas con licenciamiento GPL, los cuales cuentan con muchos años de desarrollo, cuentan con una comunidad que los soporta y evita el pago de costosas licencias de uso.

BIBLIOGRAFÍA

ASTUDILLO, Karina. Hacking ético 101. (2013) [Consultado el 01 de septiembre de 2020] Libro electrónico disponible en: https://eduarmandov.files.wordpress.com/2017/05/security-hacking-etico-101.pdf

BANACH, Zbigniew (2019) Red Team Vs Blue Team Testing for Cybersecurity. Disponible en: https://www.netsparker.com/blog/web-security/red-team-vs-blue-team/

BERTINO, E. (2012). Data Protection from Insider Threats. Morgan & Claypool. Edition 1, 2012.

CAROZO B, Eduardo. (2013) Centro de Respuesta a Incidentes Informáticos… ¿Para qué? Revista SEGURIDAD No.1 6 / enero-febrero 2013 ISSN: 1 251 478. [Consultado el 2 de Octubre de 2020] Disponible en: https://revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/Seguridad_Num16_0.pdf

Cisco. (2020). What Is Cybersecurity? - Cisco. Cisco.Com. Disponible en: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

CISET. (2020) ¿Qué es el hardening de sistemas operativos? [Consultado el 1 de octubre de 2020] Disponible en: https://www.ciset.es/publicaciones/blog/746-hardening

COLOMBIA. COPNIA – Código de Ética para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares. [Consultado el 07 de septiembre de 2020] Disponible en: https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

COLOMBIA – SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Ley 1273 de 2009 – ley de delitos informáticos [Consultado el 10 de septiembre de 2020] Disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Elasticsearch: Search & Analyze Data in Real Time. (2015). – Elasticsearch. USA. Disponible en: https://www.elastic.co/products/elasticsearch

ESET. ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes? (2015) [Consultado el 2 de octubre de 2020] Disponible en: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

GAVIRIA, Raúl. Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0 (2015). Unilibre Pereira. [Consultado el 18 de septiembre 2020] Disponible en: http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1

ORMAN Hilarie. (2013). The Compleat Story of Phish. IEEE. Disponible en: https://ieeexplore.ieee.org/document/6415920

OWASP. Equipo de respuesta a incidentes informáticos. CESICAT. [Consultado el 2

de Octubre de 2020]. Disponible en: https://owasp.org/www-pdf-archive//OWASPSpain8_CESICAT_Equipo_de_Repuesta_a_Incidentes.pdf

RAMOS V, Antonio. Seguridad perimetral, monitorización y ataques en redes. (2013) Ediciones de la U.

REVISTA SEMANA, ¿Qué se ha encontrado hasta ahora? Publicado el 2 de agosto de 2014. [Consultado el 11 de septiembre de 2020] Disponible en: https://www.semana.com/nacion/articulo/chuzadas-lo-que-se-ha-encotrado/376549-3/

STALLING, William. Fundamentos de Seguridad en Redes – Aplicaciones y Estándares. (2014) Ed. Prentice Hall.

TORI, Carlos. Hacking Ético. (2008) Liberado por el autor. [Consultado el 02 de septiembre de 2020] Disponible en: https://nebul4ck.files.wordpress.com/2015/08/hacking-etico-carlos-tori.pdf